Retrodirective assisted secure wireless key establishment

Retrodirective-Assisted Secure Wireless Key Establishment

Yuan Ding, Junqing Zhang, and Vincent F. Fusco, *Fellow, IEEE*

***Abstract*— In this paper, a new type of architecture for secure wireless key establishment is proposed. A retrodirective array (RDA) that is configured to receive and re-transmit at different frequencies is utilized as a relay node. The RDA is able to respond in "real time," reducing the required number of time slots to two. More importantly, in this architecture, equivalent reciprocal wireless channels between legitimate keying nodes can be randomly updated within one channel coherence time period, leading to greatly increased key generation rates in slow fading environment. The secrecy performance of this RDA-assisted key generation system is evaluated under several eavesdropping strategies and it is shown that it outperforms previous relay key generation systems.**

***Index Terms*— Retrodirective array, key generation, wireless communication.**

I. Introduction

MOBILE wireless communication has experienced an unprecedented growth in recent years presenting many enterprise opportunities. Along with these opportunities there are attendant risks. The broadcast nature of the electromagnetic wave propagation medium in a wireless environment significantly increases the chances of sensitive information being intercepted by eavesdroppers. Currently sensitive transmission data is encrypted at the upper protocol layers through mathematical cryptographic means [1]. Recently the potential for the efficacy of such mathematical encryption schemes to be mitigated has been under discussion [2]. Furthermore, requirements related to trusted key management infrastructure may render conventional cryptographic method less applicable for some wireless systems, such as ad-hoc networks and low-cost wireless sensor networks [3], hence potentially providing a systemic issue regarding ubiquitous rollout of the Internet of Things [4].

Distinct from the upper layer cryptographic approach, physical layer security techniques do not reply on computational complexity. This implies that the achieved level of security will not be compromised even if an unauthorized third party has unlimited computational capability [5]. One form of physical layer security techniques relies on the establishment of secret keys by exploiting randomness of reciprocal propagation channels between keying nodes [6], [7]. The information theoretical foundation of this key establishment approach was given in [8] and [9].

Key generation normally consists of four steps: channel probing, quantization, information reconciliation, and privacy amplification [7]. Two legitimate users alternately measure the signal waveforms transmitted through propagation channels to harvest the randomness in channel probing stage. After converting the channel measurements into binary bits in quantization step, the mismatch bits of shared keys are corrected in information reconciliation using protocols or error correction codes. Finally the leaked information on shared keys is removed in privacy amplification step, e.g., through universal hashing functions. In this paper, we focus on designing a relay-based key generation architecture which enables a larger amount of common information being shared among keying nodes in wireless channel probing stage, when compared with previous relay key generation schemes. The remaining key generation procedures investigated previously, e.g., quantization schemes in [10], information reconciliation in [11], and privacy amplification in [12], can then be implemented after the common signal waveforms have been obtained in the channel probing stage.

There are several characteristics of legitimate channels that can be utilized to extract secret keys, such as received signal strength (RSS) [13]–[15], channel phase delays [16], [17], multipath relative time delays [18], [19], and full channel state information (CSI) [20], [21]. No matter which channel parameters are chosen, there is always a trade-off between key generation rate (KGR), describing the amount of key bits generated per time unit, and key disagreement rate (KDR), denoting bit disagreement rates of the generated keys shared by legitimate nodes. In a slow fading channel, the channel cross-correlation is impacted by the non-simultaneous probing and independent noise at each keying node, which result in the key disagreement [21], [22]. Therefore, the number of key quantization levels should be kept small in order to get a low KDR. On the other hand, slow fading channels and low quantization levels limit achievable KGR, since the key generation round can only be conducted once during one channel coherence time period.

A number of approaches have been proposed to increase KGR without degrading KDR. In [15], [23], and [24] multiple

Manuscript received May 6, 2016; revised August 23, 2016, October 5, 2016; accepted October 6, 2016. Date of publication October 11, 2016; date of current version January 13, 2017. This work was supported by the EPSRC of UK under Grant EP/N020391/1. The associate editor coordinating the review of this paper and approving it for publication was Z. Ding.

The authors are with the Institute of Electronics, Communications and Information Technology, Queen's University of Belfast, Belfast, BT7 1NN, U.K. (e-mail: yding03@qub.ac.uk; jzhang20@qub.ac.uk; v.fusco@ecit.qub.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2016.2616406

nodes or multiple antennas at each node are exploited in order to create multiple usable common channels from which more key bits can be extracted within one channel coherence time period. Similarly, multiple independent or quasi-independent channels can be generated using frequency resources, such as channel hopping in [25]–[27], and OFDM signals in [21] and [28]–[30]. A concept utilizing random beamforming was proposed in [27], [31], and [32]. Here the excitation weights of multi-antenna nodes are randomly updated during each key generation round, such that a controlled artificial 'fast fading' channel is created. As a consequence, more independent random secret key bits can be generated by repeated channel probing within one channel coherence time period.

In addition to the above methods, helper or relay nodes have been introduced in [17] and [33]–[37]. In [33] the presence of a relay node helps create two more common channels that exist between each of the keying nodes and the relay, such that KGR can be increased. Apart from creating more usable channels, the relay nodes can also help generate artificial noise [34], [35], which contaminates the intercepted signals received by eavesdroppers, or helps enhance the randomness of the channel characteristics, [35]–[37], in such a fashion to increase secret key rates. However, there are issues associated with the helper or relay architectures, which are listed as follows:

a) the relay or helper needs to have calculation capabilities, e.g., estimating channels in [33], generating well designed artificial interference in [34], [35], and demodulating signals in [37];
b) the relay or helper needs to be a trusted party [17], [34]–[36], and in some cases a secure channel between helper and one of the keying nodes is required [34];
c) the relay or helper has to acquire some system knowledge before carrying out key generation protocols. This includes time-slot assignment [17], [33]–[37], CSI of legitimate channels [17], and the training symbols used in the system [33], [35], [36];
d) only one probing of the channel can be performed per coherence time period [17], [33]–[37].

These factors make the above mentioned relay key generation architectures unsuitable in many application scenarios.

In this paper we propose a new type of relay key generation architecture, which uses a retrodirective array (RDA) [38] as a relay node. By configuring the RDA node to receive and re-transmit at different frequencies, the common waveform observations can be shared among legitimate users for further secret key extraction. This arrangement has the following characteristics that facilitate overcoming the above mentioned weaknesses;

a) the RDA relay node can be implemented in an analogue fashion thereby allowing low power consumption and the real-time response. The RDA node does not need to have any additional digital calculation capabilities;
b) no secure links between RDA and other keying nodes are required. Since the RDA can operate without demodulating signals nor estimating channels, the potential for the relay node to leak information intentionally or unintentionally is significantly reduced, i.e., it can be considered as a trusted node;
b) no system parameters including CSI, training sequences, and time-slot assignment are required by the RDA relay node;
d) multiple channel measurements can be conducted within one coherence time period, because with the help of the RDA the equivalent channel can be manipulated to be 'fast fading', greatly increasing the achievable KGR.

Besides the above listed characteristics, the proposed architecture requires only two time slots for each key generation round, compared with at least three time slots in previous relay key generation protocols.

We need to point out that the approaches presented in [21]–[32], i.e., multi-antenna, multi-carrier, and ramdom beamforming schemes, can also be applied onto the RDA key generation architecture proposed in this paper, leading to a further increased KGR. The combinations of these techniques with the methodology suggested here are not discussed in this paper.

This paper is organized as follows;

- In Section II, system models including statistical multipath channels and RDAs used throughout the paper are described.
- In Section III, the single antenna element RDA assisted key generation architecture and the protocol deployed are presented. In additional, various strategies with minimum assumptions that can be adopted by eavesdroppers are discussed.
- In Section IV, the secret key rates of the proposed system are simulated and compared with non-relay and previous relay key generation systems. It is shown that the proposed RDA assisted key generation system outperforms the previous relay key generation systems under every eavesdropping scenarios, in terms of secrecy performance.
- In Section V, from a more practical point of view the impact of imperfect training sequence recovery at each node on the system performance is investigated.
- In Section VI, the benefits of higher beamforming gains towards legitimate nodes than those towards eavesdroppers, which are brought by involving more antenna elements in RDA relay nodes, are briefly investigated.
- In Section VII, conclusions are drawn.

Throughout this paper, the following notations will be used: Boldface lower case and capital letters, e.g., $\boldsymbol{h}$ and $\boldsymbol{H}$, denote parameters in time and frequency domains, respectively, and they are complex numbers. Boldface capital letter with an arrow on top refers to a vector, whose elements are parameters in frequency domain. Letters with superscripts RDA, nr, and r correspond to parameters in the proposed RDA, non-relay, and previous relay key generation systems. '$[\cdot]^*$' denotes complex conjugate operator, and '$\circ$' is the Hadamard product of two vectors. '$[x]^+$' returns zero if x is less than zero otherwise returns x.

II. System Model

A. Statistical Multipath Channel Model

In this paper a dynamic multipath-rich Rayleigh wireless propagation channel is considered. The channel impulse response (CIR) can be written as

$$\boldsymbol{h}(\tau, t) = \sum_{l=0}^{L-1} \boldsymbol{h}(\tau_l, t)\delta(\tau - \tau_l), \tag{1}$$

where $\boldsymbol{h}(\tau_l, t)$ is a complex number representing the attenuation and phase delay of the l^{th} $(l = 0, 1, ..., L-1)$ propagation path, i.e., channel taps, between communication nodes at the time instant t. τ_l refers to the time delay of the l^{th} channel tap relative to the corresponding t. $\delta(\cdot)$ is the Dirac delta function. It is assumed that, a) at each time instant the total number of channel taps, i.e., L, is identical, b) τ_l starts from zero and is uniformly spaced in time. Thus it can be expressed as $\tau_l = lT$, where T is normally determined by the sampling period of the hardware, c) the scattering multipath in the channel is sufficiently rich that the $\boldsymbol{h}(\tau_l, t)$ follows zero-mean complex Gaussian distribution, i.e., $\boldsymbol{h}(\tau_l, t) \sim CN(0, \sigma_{hl}^2)$ [39].

When taking Fourier transform of (1) with respect to τ, the channel frequency response (CFR) can be obtained, and is given as

$$\boldsymbol{H}(f, t) = \sum_{l=0}^{L-1} \boldsymbol{h}(\tau_l, t)e^{-j2\pi f \tau_l}. \tag{2}$$

Unless otherwise specified, all of the simulation results presented in this paper are based on the following channel parameters for typical wireless indoor environment [40].

- The sampling period T is set to 50 ns;
- The average power of each channel tap follows an exponential decay power delay profile with root mean square (RMS) delay spread σ_τ of 50 ns, from which the number of channel taps can be calculated to be 11;
- A bell-shaped Doppler power spectral density with Doppler spread f_d of 10 Hz is used.

The normalized auto-correlation function (ACF) of $\boldsymbol{H}(f, t)$ can be formulated as [41]

$$r_H(\Delta f, \Delta t) = \frac{E\left[\boldsymbol{H}^*(f, t)\,\boldsymbol{H}(f + \Delta f, t + \Delta t)\right]}{E\left[\boldsymbol{H}^*(f, t)\,\boldsymbol{H}(f, t)\right]}, \tag{3}$$

where '$E[\cdot]$' is the expectation operator. From the ACF the channel's coherence bandwidth f_c and coherence time T_c can be calculated [42].

B. Retrodirective Arrays (RDAs)

Before describing the RDA relay key generation system in Section III, RDA operation is briefly presented here. An RDA has the capability to re-transmit a signal back along the spatial direction(s), along which the array was illuminated by the incoming signals without the need for a-priori knowledge of their points of origin [38]. This automatic tracking characteristic makes RDA technology useful in many mobile applications, e.g., long-range radio frequency identification (RFID) [43] and mobile satellite communications [44], [45]. The core element of an RDA that enables the tracking functionality is the phase conjugator unit [46]. Among many forms of phase conjugator units, active analogue types are attractive due to their low power consumption, real-time response, and frequency reconfiguration flexibility [47], [48].

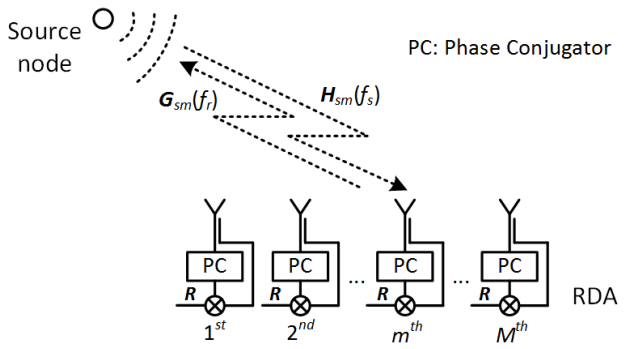


Fig. 1. RDA operating principle.

The basic operation upon which an RDA is predicated is illustrated by way of an example shown in Fig. 1. A distant source emits a pilot signal $\boldsymbol{s}(t)$, which can be a radio frequency (RF) continuous wave (CW) or a modulated signal waveform [49], at frequency f_s. The detected signal in the frequency domain at the m^{th} $(m = 1, 2, ..., M)$ RDA element can be expressed as $\boldsymbol{S}(f_s)\boldsymbol{H}_{sm}(f_s)$, where the $\boldsymbol{S}(f_s)$ and $\boldsymbol{H}_{sm}(f_s)$ are, respectively, the Fourier representations of the pilot signal $\boldsymbol{s}(t)$ and the propagation channel $\boldsymbol{h}_{sm}(t)$ between the source and the m^{th} RDA antenna element. After the detected signal is processed through a phase conjugator, it becomes $[\boldsymbol{S}(f_s)\boldsymbol{H}_{sm}(f_s)]^*$. When re-transmitting $[\boldsymbol{S}(f_s)\boldsymbol{H}_{sm}(f_s)]^*$ weighted local signal $\boldsymbol{C}$ at frequency f_r by the RDA, the received signal $\boldsymbol{Y}(f_r)$ at the source node can be written as in (4),

$$\boldsymbol{Y}(f_r) = \sum_{m=1}^{M} \boldsymbol{C}[\boldsymbol{S}(f_s)\boldsymbol{H}_{sm}(f_s)]^*\boldsymbol{G}_{sm}(f_r). \tag{4}$$

A well-designed analogue RDA is able to complete the phase conjugation operation within 100 μs, which is normally much less than the channel coherence time T_c (usually in the order of tens or hundreds of ms in indoor environment). Thus the re-transmission channel $\boldsymbol{G}_{sm}(f_r)$ can be normally regarded to be identical to the reception channel $\boldsymbol{H}_{sm}(f_s)$ when $f_r = f_s$. In this case (4) can, in the absence of noise, be expressed as

$$\boldsymbol{Y}(f_s) = \boldsymbol{C}\boldsymbol{S}^*(f_s) \sum_{m=1}^{M} |\boldsymbol{H}_{sm}(f_s)|^2 . \tag{5}$$

Equation (5) indicates that the re-transmitted signals by each RDA element are combined constructively both spatially and temporally or, in other words, in-phase at the source node, i.e., automatically re-transmitting signal back to the source position where the pilot signal is originated.

When $f_r \neq f_s$, as occurs in full-duplex RDAs, the re-transmission channel $\boldsymbol{G}_{sm}(f_r) \neq \boldsymbol{H}_{sm}(f_s)$. In free space $\boldsymbol{G}_{sm}(f_r)$ and $\boldsymbol{H}_{sm}(f_s)$ can be directly linked by compensating their frequency differences [50], thus after channel coefficient

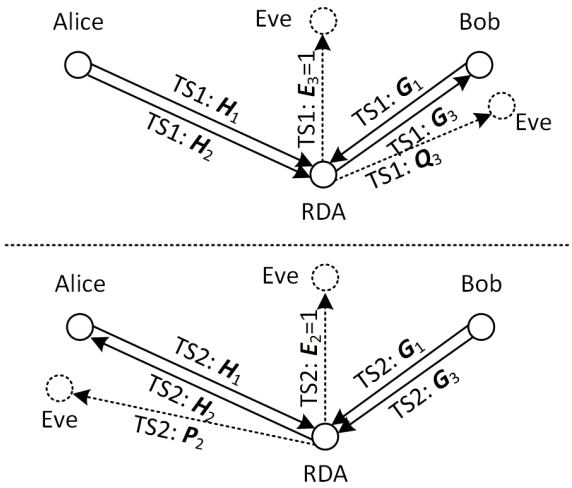


Fig. 2. Proposed RDA assisted wireless key generation system model.

calibration (5) still holds. The scenario of RDAs in multipath channels when $f_r \neq f_s$ is investigated in Section VI.

When an RDA is illuminated by multiple pilot sources from different directions, as occurs in our proposed system architecture described in Section III, the signals are re-transmitted along all of these directions with their beamforming gains proportional to the magnitudes of the corresponding received pilot signals along these directions [51]. This scenario is essentially equivalent to the case of single pilot source in a multipath environment.

III. RDA Assisted Wireless Key Generation

In this section single antenna RDA assisted key generation system is presented and the associated adversary model is investigated. It should be noted that the single antenna RDA is still able to phase conjugate the incoming signal, but cannot perform beamforming for re-transmission towards the pilot source. This architecture is further extended to the multi-antenna RDA key generation system in Section VI with additional benefits presented.

A. Single Antenna RDA Assisted Key Generation

The model of the proposed single antenna RDA assisted key generation system is illustrated in Fig. 2. The nodes Alice and Bob intend to establish a shared common key with the help of a single antenna RDA node. These three nodes are termed legitimate nodes hereafter. In this paper we assume Alice and Bob are both equipped with a single antenna. Not discussed in this paper are multiple-antenna cases which can be investigated using similar methods to those in [23] and [52] for MIMO key generation scenarios.

Each key generation round only comprises two time slots (**TS**1, 2), which are now described;

TS1) Alice and Bob locally generate random and independent signals $\boldsymbol{U}_i$ and $\boldsymbol{V}_i$, respectively, and then radiate them at an identical frequency f_1. Here the subscript 'i' refers to the i^{th} key generation round. In order to simplify notation, the subscript 'i' is omitted later in most cases. In order to facilitate signal to noise ratio (SNR) definition later in Section IV, it is assumed that $E[\boldsymbol{U}] = E[\boldsymbol{V}] = 0$, and $E\big[|\boldsymbol{U}|^2\big] = E\big[|\boldsymbol{V}|^2\big] = 1$. Alice and Bob do not need to know or store the values of $\boldsymbol{U}$ and $\boldsymbol{V}$. The detected signal $\boldsymbol{W}_b$ at the RDA element can be expressed as

$$\boldsymbol{W}_b = q_{1b}^{1/2}(\boldsymbol{H}_1\boldsymbol{U} + \boldsymbol{G}_1\boldsymbol{V}) + \boldsymbol{N}_{1b}, \tag{6}$$

where $\boldsymbol{H}_x$ ($\boldsymbol{G}_x$) represents the channel coefficient between Alice (Bob) and the RDA element at frequency f_x ($x = 1, 2, 3$), see Fig. 2. $\boldsymbol{N}_{xy}$ ($y = a, b$) is the frequency representation of the additive white Gaussian noise (AWGN) $n_{xy} \sim CN(0, \sigma_n^2)$, and all are independent. $q_{xy}^{1/2}$ is a scaling coefficient involving both the amplification factor at transmitter sides and propagation path loss, and it is used to set required SNR at receiver sides. Here the $E\big[\,|\boldsymbol{H}_1\boldsymbol{U} + \boldsymbol{G}_1\boldsymbol{V}|^2\,\big]$ is normalized to be unity. The RDA cannot separate the two signals transmitted by Alice and Bob because both signals are at the same frequency, and are occurring at the same time, and none of $\boldsymbol{H}_1$, $\boldsymbol{G}_1$, $\boldsymbol{U}$, and $\boldsymbol{V}$ are known.

At the same time Alice transmits a publicly known training sequence $\boldsymbol{X}$ at a different frequency f_2 ($f_2 \neq f_1$). The received signal at the RDA element at frequency f_2 is $q_{2b}^{1/2}\boldsymbol{H}_2\boldsymbol{X} + \boldsymbol{N}_{2b}$. Here $\boldsymbol{H}_2$ is normalized such that $E\big[|\boldsymbol{H}_2|^2\big] = 1$, seen in Fig. 2. Then the $\boldsymbol{W}_b^*$ weighted $q_{2b}^{1/2}\boldsymbol{H}_2\boldsymbol{X}+\boldsymbol{N}_{2b}$ is radiated by the RDA element at frequency f_3 ($f_3 \neq f_2$, $f_3 \neq f_1$).

At the Bob the detected signal $\boldsymbol{S}_b$ at frequency f_3 can be written as

$$\boldsymbol{S}_b = q_{3b}^{1/2}\boldsymbol{G}_3\boldsymbol{W}_b^*\left(q_{2b}^{1/2}\boldsymbol{H}_2\boldsymbol{X} + \boldsymbol{N}_{2b}\right) + \boldsymbol{N}_{3b}. \tag{7}$$

Similarly $\boldsymbol{G}_3$ is normalized to be $E[|\boldsymbol{G}_3|^2] = 1$.

Since $\boldsymbol{X}$ is publicly known to every node in the system, Bob is able to obtain the waveform observation $\boldsymbol{K}_b$, which in the frequency domain for the purpose of secret key extraction is shown in (8).

$$\boldsymbol{K}_b = q_{3b}^{1/2}q_{2b}^{1/2}\boldsymbol{G}_3\boldsymbol{W}_b^*\boldsymbol{H}_2 + q_{3b}^{1/2}\boldsymbol{G}_3\boldsymbol{W}_b^*\boldsymbol{N}_{2b}\big/\boldsymbol{X} + \boldsymbol{N}_{3b}\big/\boldsymbol{X} \tag{8}$$

TS2) In time slot 2, $\boldsymbol{U}$ and $\boldsymbol{V}$ transmitted by Alice and Bob at frequency f_1 are still present, which generates $\boldsymbol{W}_a$ at the RDA node, seen in (9).

$$\boldsymbol{W}_a = q_{1a}^{1/2}\,(\boldsymbol{H}_1\boldsymbol{U} + \boldsymbol{G}_1\boldsymbol{V}) + \boldsymbol{N}_{1a} \tag{9}$$

In this time slot Bob transmits the same known $\boldsymbol{X}$ at frequency f_3, which, after being weighted with $\boldsymbol{W}_a^*$, is re-transmitted by the RDA at frequency f_2. When the known $\boldsymbol{X}$ is equalized, the waveform $\boldsymbol{K}_a$ shown in (10) can be acquired by Alice.

$$\boldsymbol{K}_a = q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_a^*\boldsymbol{G}_3 + q_{2a}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_a^*\boldsymbol{N}_{3a}\big/\boldsymbol{X} + \boldsymbol{N}_{2a}\big/\boldsymbol{X} \tag{10}$$

From the first term of the obtained $\boldsymbol{K}_a$ in (10) at Alice node and the first term of the obtained $\boldsymbol{K}_b$ in (8) at

Bob node, a common secret key can be generated and shared. The noise terms, i.e., the last two terms in both (8) and (10), reduce the correlation coefficients between $\boldsymbol{K}_a$ and $\boldsymbol{K}_b$, and hence limit the achievable secret key rates of the proposed system. These aspects are investigated in Section IV.

It is worth pointing out that even within one channel coherence time period, i.e., $\boldsymbol{H}_1$, $\boldsymbol{G}_1$, $\boldsymbol{H}_2$, and $\boldsymbol{G}_3$ remain unchanged (here channel reciprocity is assumed), the equivalent common channel observation $\boldsymbol{H}_2\boldsymbol{W}^*_{\{a,b\}}\boldsymbol{G}_3$ still varies, and for different key generation rounds they are uncorrelated. This is achieved by randomly choosing $\boldsymbol{U}_i$ and $\boldsymbol{V}_i$, which are unknown to any of the nodes in the system, in each key generation round. In other words, many key generation rounds can be performed within one channel coherence time period, leading to a greatly increased KGR.

When compared with the conventional digital transceivers used in previous relay key generation systems, the analogue phase-locked-loop (PLL) phase conjugators [47] remove the needs of analogue-to-digital converters, digital-to-analogue converters, and digital processing units, and for appropriate frequency chosen, down-conversion and up-conversion modules can also be eliminated. In this sense, the proposed RDA relay system has lower cost. The system implementation is under way with the PLL chipset ADF4360-1 chosen. The experimental setup and measured results are planned to be reported separately.

B. Eavesdropping Strategies

In this subsection, the effects of some eavesdropping strategies that can be adopted by a malicious node, named as Eve, are investigated.

Following the same assumptions in most physical layer key generation schemes in wireless networks [13], [16], [35], we assume that:

- Eve knows the key generation procedures described in the previous subsection;
- Every nodes in the system, including Eve, know the training sequence $\boldsymbol{X}$. The case of $\boldsymbol{X}$ being obtained by actual wireless transmission is investigated in Section V.

The above is actually the worst scenario with regard to the secure wireless transmission.

In this paper, we investigate three worst-case eavesdropping strategies:

a) Eve is able to obtain the 'clean' signals that are transmitted by one of the legitimate nodes. Here the 'clean' simply means no multipath and no channel noise. In this case the channel coefficient between one of the legitimate nodes and Eve is set to 1;
b) It is assumed that Eve's antenna is able to be placed close enough to one of the legitimate nodes, which leads to correlated legitimate and eavesdropping channels;
c) The combination of the cases a) and b), i.e., Eve is able to obtain 'clean' signals transmitted by each legitimate node and Eve is able to create correlated legitimate and eavesdropping channels.

It is obvious to conclude that the strategy c) is equivalent to the case of multiple Eves that are able to collude, which is not commonly studied in previous key generation work.

We investigate the secret key rate R_s^{RDA} [9], [53], expressed in (11), for different eavesdropping strategies in our proposed RDA key generation system. '$I(\cdot;\cdot)$' denotes mutual information. Here we assume Eve attempts to estimate the generated waveform $\boldsymbol{K}_a$ ($\boldsymbol{K}_b$) at Alice (Bob) node. The estimation is denoted as $\boldsymbol{K}_e$. Only real parts of associated waveforms, i.e., $Re(\boldsymbol{K}_a)$, $Re(\boldsymbol{K}_b)$, and $Re(\boldsymbol{K}_e)$, are considered in order to facilitate comparison with previous related works [35].

$$R_s^{RDA} = \Bigg[I\Big(Re\left(\boldsymbol{K}_a\right); Re\left(\boldsymbol{K}_b\right)\Big) - min\Bigg(I\Big(Re\left(\boldsymbol{K}_a\right); Re\left(\boldsymbol{K}_e\right)\Big), I\Big(Re\left(\boldsymbol{K}_b\right); Re\left(\boldsymbol{K}_e\right)\Big)\Bigg)\Bigg]^+ \tag{11}$$

a) Eve observes one of the legitimate nodes.
   - *Eve intercepts the signals radiated by Alice.* Alice radiates signals at frequencies f_1 and f_2. If Eve has ability to intercept at both frequencies, she can obtain $\boldsymbol{U}$ and the publicly known $\boldsymbol{X}$.
   - *Eve intercepts the signals radiated by Bob.* Bob radiates signals at frequencies f_1 and f_3. If Eve has ability to intercept at both frequencies, she can obtain $\boldsymbol{V}$ and the publicly known $\boldsymbol{X}$.
   - *Eve intercepts the signals radiated by the RDA.* In **TS**1 RDA radiates signals at frequency f_3. The noiseless observation, after $\boldsymbol{X}$ being divided, is

   $$\boldsymbol{K}_e^{\mathbf{TS}1} = q_{3b}^{1/2} q_{2b}^{1/2} \boldsymbol{W}_b^* \boldsymbol{H}_2 + q_{3b}^{1/2} \boldsymbol{W}_b^* \boldsymbol{N}_{2b} \big/ \boldsymbol{X}. \tag{12}$$

   Similarly, in **TS**2 RDA radiates signals at frequency f_2. The noiseless observation, after $\boldsymbol{X}$ being divided, is

   $$\boldsymbol{K}_e^{\mathbf{TS}2} = q_{2a}^{1/2} q_{3a}^{1/2} \boldsymbol{W}_a^* \boldsymbol{G}_3 + q_{2a}^{1/2} \boldsymbol{W}_a^* \boldsymbol{N}_{3a} \big/ \boldsymbol{X}. \tag{13}$$

   When comparing $\boldsymbol{K}_e^{\mathbf{TS}\{1,2\}}$ and $\boldsymbol{K}_{\{a,b\}}$, it can be concluded that Eve has three choices to estimate legitimate waveforms. They are $\boldsymbol{K}_e^{\mathbf{TS}1}$, $\boldsymbol{K}_e^{\mathbf{TS}2}$, and $\boldsymbol{K}_e^{\mathbf{TS}1}\boldsymbol{K}_e^{\mathbf{TS}2}$.

   It is obvious that Eve can acquire more information for better estimation of the $\boldsymbol{K}_{\{a,b\}}$ through observing the signals transmitted by the RDA, compared with the amount of information obtained through intercepting Alice (Bob)'s signal radiation.
b) Eve's antenna is placed close enough to one of the legitimate nodes.
   - *Eve's antenna is placed close to Alice.* In this case the eavesdropping channel between Eve and the RDA is correlated to the legitimate channel between Alice and the RDA. Since the RDA radiates signals at frequencies f_2 and f_3 in two different time slots, two pairs of correlating channels are created. One pair of correlating channels at frequency f_3 are denoted as $\boldsymbol{P}_3$ and $\boldsymbol{H}_3$, respectively, for eavesdropping and legitimate channels. However, since

the legitimate channel $\boldsymbol{H}_3$ is not utilized in key generation process, see (8) and (10), this channel pair does not help Eve in terms of interception. The other eavesdropping channel at frequency f_2, denoted as $\boldsymbol{P}_2$, is correlated to $\boldsymbol{H}_2$ through the correlation coefficient ρ_{ae}^{RDA} expressed in (14).

$$\rho_{ae}^{RDA} = \frac{E\left(Re(\boldsymbol{P}_2)Re(\boldsymbol{H}_2)\right)}{\sqrt{E\left[\left(Re(\boldsymbol{P}_2)\right)^2\right]E\left[\left(Re(\boldsymbol{H}_2)\right)^2\right]}} \quad (14)$$

Eve cannot estimate $\boldsymbol{P}_2$, and hence $\boldsymbol{H}_2$, since $q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{W}_a^*\boldsymbol{G}_3\boldsymbol{X}+q_{2a}^{1/2}\boldsymbol{W}_a^*\boldsymbol{N}_{3a}$ radiated by the RDA in **TS**2 is unknown to any nodes in the system. Fortunately, from Eve's point of view, she does not need to know $\boldsymbol{H}_2$. It is better for her to estimate $\boldsymbol{K}_a$ as a whole directly. The obtained waveform, $\boldsymbol{K}_e^{ae}$, used for estimation can be written as

$$\boldsymbol{K}_e^{ae} = q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{P}_2\boldsymbol{W}_a^*\boldsymbol{G}_3 + q_{2a}^{1/2}\boldsymbol{P}_2\boldsymbol{W}_a^*\boldsymbol{N}_{3a}/\boldsymbol{X} + \boldsymbol{N}_{2e}^{ae}/\boldsymbol{X}, \quad (15)$$

where channel noise $\boldsymbol{N}_{2e}^{ae}$ at the Eve node is assumed to have the same distribution as $\boldsymbol{N}_{2a}$.

- *Eve's antenna is placed close to Bob.*
  Similar to the case discussed above, an eavesdropping channel, denoted as $\boldsymbol{Q}_3$, is created at frequency f_3, and it is correlated to the legitimate channel $\boldsymbol{G}_3$ with a correlation coefficient ρ_{be}^{RDA}. ρ_{be}^{RDA} is expressed the same as ρ_{ae}^{RDA} in (14) with $\boldsymbol{P}_2$ and $\boldsymbol{H}_2$ being replaced with $\boldsymbol{Q}_3$ and $\boldsymbol{G}_3$, respectively.
  The corresponding waveforms, $\boldsymbol{K}_e^{be}$, used for estimation at Eve node can be expressed in

$$\boldsymbol{K}_e^{be} = q_{3b}^{1/2}q_{2b}^{1/2}\boldsymbol{Q}_3\boldsymbol{W}_b^*\boldsymbol{H}_2 + q_{3b}^{1/2}\boldsymbol{Q}_3\boldsymbol{W}_b^*\boldsymbol{N}_{2b}/\boldsymbol{X} + \boldsymbol{N}_{3e}^{be}/\boldsymbol{X}, \quad (16)$$

  where channel noise $\boldsymbol{N}_{3e}^{be}$ at the Eve node is assumed to have the same distribution as $\boldsymbol{N}_{3b}$.
- *Eve's antenna is placed close to the RDA.*
  In this case Eve is able to obtain an estimation of $\boldsymbol{H}_2$ and $\boldsymbol{G}_3$, since Alice and Bob project $\boldsymbol{X}$ at frequency f_2 and f_3, respectively. It is noted that although Alice and Bob transmit $\boldsymbol{U}$ and $\boldsymbol{V}$ at frequency f_1, the corresponding channels, $\boldsymbol{H}_1$ and $\boldsymbol{G}_1$, cannot be estimated by Eve. This is because $\boldsymbol{U}$ and $\boldsymbol{V}$ are transmitted at the same frequency at the same time and they are unknown to any of the nodes in the system. The leakage of parts of $\boldsymbol{H}_2$ and $\boldsymbol{G}_3$ helps little to Eve in terms of interception, compared with the strategies of placing the antenna close to Alice or Bob discussed above.

c) Multiple Eves that are able to collude.
It is obvious that this case of multiple colluding Eves includes the scenarios a) and b) discussed above. As a consequence, the secrecy performance in this case is upper bounded by those obtained under the scenarios a) and b). In this subsection, we investigate a straightforward strategy that can be adopted by colluding Eves, i.e., collaboratively estimate each factor within $q_{2\{b,a\}}^{1/2}q_{3\{b,a\}}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_{\{b,a\}}^*\boldsymbol{G}_3$, which are the first items in $\boldsymbol{K}_{\{b,a\}}$, respectively, and which are used for common secret key extraction. In order to simplify discussion, only the eavesdropping of $q_{2b}^{1/2}q_{3b}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_b^*\boldsymbol{G}_3$ in **TS**1 is studied. The case of eavesdropping of $q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_a^*\boldsymbol{G}_3$ in **TS**2 can be formulated similarly.
The three factors within $q_{2b}^{1/2}q_{3b}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_b^*\boldsymbol{G}_3$ can be estimated as follows,

- Estimation of $q_{2b}^{1/2}\boldsymbol{H}_2$.
  There are two ways of estimating $\boldsymbol{H}_2$. Eve can place her antenna either close to Alice or close to the RDA, creating a pair of correlating channels $\boldsymbol{P}_2$ and $\boldsymbol{H}_2$ or $\boldsymbol{J}_2$ and $\boldsymbol{H}_2$. $\boldsymbol{J}_2$ is the channel coefficient between Alice and the Eve that is close to the RDA. Since in the key generation process Alice transmits publicly known $\boldsymbol{X}$ at f_2 in **TS**1, while the RDA transmits noisy unknown $\boldsymbol{W}_a^*\boldsymbol{G}_3$ at f_2 in **TS**2, it is obvious that placing Eve's antenna close to the RDA, i.e., estimating $\boldsymbol{H}_2$ via the calculation of $\boldsymbol{J}_2$, is the better strategy that Eve should adopt. The correlation coefficient between $\boldsymbol{J}_2$ and $\boldsymbol{H}_2$ is denoted as ρ_{e2}^{RDA}. In this case the estimation of $q_{2b}^{1/2}\boldsymbol{H}_2$ can be expressed as

$$q_{2b}^{1/2}\hat{\boldsymbol{H}}_2 = q_{2b}^{1/2}\boldsymbol{J}_2 + \boldsymbol{N}_{2e}^{re}/\boldsymbol{X}, \quad (17)$$

  where the noise $\boldsymbol{N}_{2e}^{re}$ is assumed to have the same distribution as $\boldsymbol{N}_{2b}$.
- Estimation of $q_{3b}^{1/2}\boldsymbol{G}_3$.
  Similarly the best estimation can be obtained in **TS**2 by an Eve whose antenna is placed close to the RDA. In this case a pair of correlating channels $\boldsymbol{J}_3$ and $\boldsymbol{G}_3$ with correlation coefficient ρ_{e3}^{RDA} is created. $\boldsymbol{J}_3$ is the channel coefficient between Bob and the Eve that is close to the RDA. The estimation of of $q_{3b}^{1/2}\boldsymbol{G}_3$ can be formulated as

$$q_{3b}^{1/2}\hat{\boldsymbol{G}}_3 = q_{3b}^{1/2}\boldsymbol{J}_3 + \boldsymbol{N}_{3e}^{re}/\boldsymbol{X}, \quad (18)$$

  where the noise $\boldsymbol{N}_{3e}^{re}$ is assumed to have the same distribution as $\boldsymbol{N}_{3a}$.
- Estimation of $\boldsymbol{W}_b$.
  $\boldsymbol{W}_b$ is shown in (6). $\boldsymbol{U}$ and $\boldsymbol{V}$ can be observed directly because under this colluding eavesdropping strategy we assume that Eve can obtain noiseless copies of signals transmitted by every legitimate nodes. However, Eve cannot separately estimate $\boldsymbol{H}_1$ and $\boldsymbol{G}_1$ since $\boldsymbol{H}_1\boldsymbol{U}$ and $\boldsymbol{G}_1\boldsymbol{V}$ are radiated at the same frequency f_1 and are occurring at the same time. As a consequence, Eve can only obtain the estimated $\boldsymbol{W}_b$ via

$$\hat{\boldsymbol{W}}_b = q_{1b}^{1/2}\left(\boldsymbol{J}_{H1}\boldsymbol{U} + \boldsymbol{J}_{G1}\boldsymbol{V}\right) + \boldsymbol{N}_{1e}, \quad (19)$$

  where the noise term $\boldsymbol{N}_{1e}$ is assumed to have the same distribution as $\boldsymbol{N}_{1b}$ in (6). $\boldsymbol{J}_{H1}$ ($\boldsymbol{J}_{G1}$) is the channel coefficient at the frequency f_1 between Alice (Bob) and the Eve whose antenna is placed close to the RDA.

With the colluding capability, multiple Eves are able to use (17), (18), and (19) to construct estimated $\boldsymbol{K}_e^{col}$,

$$\begin{aligned}\boldsymbol{K}_e^{col} &= q_{3b}^{1/2} q_{2b}^{1/2} \hat{\boldsymbol{G}}_3 \hat{\boldsymbol{W}}_b^* \hat{\boldsymbol{H}}_2 \\ &= q_{3b}^{1/2} q_{2b}^{1/2} \boldsymbol{J}_3 \hat{\boldsymbol{W}}_b^* \boldsymbol{J}_2 + q_{3b}^{1/2} \boldsymbol{J}_3 \hat{\boldsymbol{W}}_b^* \boldsymbol{N}_{2e}^{re}/X \\ &\quad + q_{2b}^{1/2} \boldsymbol{J}_2 \hat{\boldsymbol{W}}_b^* \boldsymbol{N}_{3e}^{re}/X + \hat{\boldsymbol{W}}_b^* \boldsymbol{N}_{2e}^{re} \boldsymbol{N}_{3e}^{re}/X^2. \end{aligned} \quad (20)$$

When comparing (20) with (16), it can be seen that $\boldsymbol{K}_e^{col}$ contains less information about the genuine waveform, i.e., $I\left(\boldsymbol{J}_3 \hat{\boldsymbol{W}}_b^* \boldsymbol{J}_2; \boldsymbol{G}_3 \boldsymbol{W}_b^* \boldsymbol{H}_2\right) < I\left(\boldsymbol{Q}_3 \boldsymbol{W}_b^* \boldsymbol{H}_2; \boldsymbol{G}_3 \boldsymbol{W}_b^* \boldsymbol{H}_2\right)$. Here $\boldsymbol{J}_3$ and $\boldsymbol{Q}_3$ defined early in this section are not the same, but they are equivalent. While the three noise terms in (20) are greater than the two noise terms in (16). As a consequence, we can conclude that separately estimating each factors within the waveforms shared among legitimate nodes by colluding Eves does not help eavesdropping when compared with the case b).

From the above discussions in this subsection, it can be concluded that the best strategies that Eve can adopt are directly intercepting signals radiated by the RDA, or placing Eve's antenna close enough to Alice or Bob in order to create correlated channel pairs, i.e., $\boldsymbol{P}_2$ and $\boldsymbol{H}_2$, and $\boldsymbol{Q}_3$ and $\boldsymbol{G}_3$, to estimate $\boldsymbol{K}_a$ or $\boldsymbol{K}_b$ directly, see illustrations in Fig. 2.

IV. Secrecy Performance Evaluation

In this section the secrecy performance of the proposed RDA assisted key generation system is evaluated, and compared with non-relay and previous relay systems.

The non-relay system, acting as a bench mark, comprises only Alice and Bob, between which the reciprocal Rayleigh channel is denoted as $\boldsymbol{H}^{nr}$. The previous relay key generation systems used for comparison are schemes described in [35]. Apart from the secret key rates expressed in (11), the correlation coefficients between obtained waveforms at Alice and Bob used for secret key extraction in different systems are also simulated and provided since these parameters are useful for practical system design. For example, quantization levels and signal pre-processing algorithms are determined by the correlation coefficients between waveform observations at Alice and Bob. The operation frequencies of the RDA for all the results presented in this section are configured to be $f_3 - f_1 = \Delta f = 2$ MHz and $f_2 - f_1 = \Delta f/2 = 1$ MHz.

A. Comparison With Non-Relay Key Generation System

In the non-relay key generation system, the waveforms acquired at Alice and Bob can be expressed as in (21) and (22), respectively.

$$\boldsymbol{K}_a^{nr} = q_{nr}^{1/2} \boldsymbol{H}^{nr} + \boldsymbol{N}_a^{nr} \quad (21)$$

$$\boldsymbol{K}_b^{nr} = q_{nr}^{1/2} \boldsymbol{H}^{nr} + \boldsymbol{N}_b^{nr} \quad (22)$$

The noise terms $\boldsymbol{N}_a^{nr}$ and $\boldsymbol{N}_b^{nr}$ are independent and follow $CN\left(0, \sigma_{nr}^2\right)$. The scaling factor $q_{nr}^{1/2}$ is utilized to set the required SNR^{nr}.

$$SNR^{nr} = \frac{q_{nr}}{\sigma_{nr}^2} \quad (23)$$

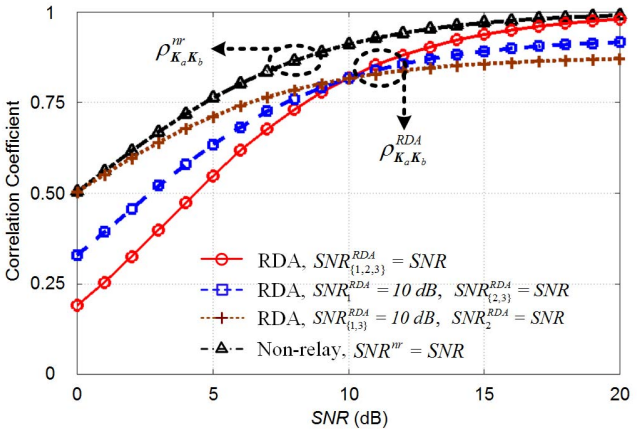


Fig. 3. Calculated correlation coefficients between observed waveforms at Alice and Bob used for secret key extraction in non-relay and proposed RDA assisted key generation systems.

In Fig. 3 the correlation coefficient $\rho^{nr}_{\boldsymbol{K}_a\boldsymbol{K}_b}$, which is calculated by replacing $\boldsymbol{P}_2$ and $\boldsymbol{H}_2$ with $\boldsymbol{K}_a^{nr}$ and $\boldsymbol{K}_b^{nr}$, respectively, in (14), is depicted as a function of SNR. Here SNR equals SNR^{nr} in (23). In simulations conducted in this paper the key generation round is repeated 4×10^6.

When bringing the proposed RDA assisted key generation system under consideration, the system SNR needs to be defined separately since more wireless communication links exist in the system. Only signal transmissions in **TS**1 are investigated. SNRs in **TS**2 can be defined in a similar way.

- The SNR of the received signals $q_{1b}^{1/2}(\boldsymbol{H}_1\boldsymbol{U} + \boldsymbol{G}_1\boldsymbol{V})$, seen in (6), at the RDA node at frequency f_1 is denoted as SNR_1^{RDA},
$$SNR_1^{RDA} = \frac{q_{1b}}{\sigma_n^2}. \quad (24)$$
It is assumed that $q_{1a} = q_{1b}$.
- The SNR of the received signals $q_{2b}^{1/2}\boldsymbol{H}_2\boldsymbol{X}$ at the RDA node at frequency f_2 is denoted as SNR_2^{RDA},
$$SNR_2^{RDA} = \frac{q_{2b}}{\sigma_n^2}. \quad (25)$$
It is assumed that $q_{2a} = q_{2b}$.
- The power ratio of the received signal $q_{1b}^{1/2} q_{2b}^{1/2} q_{3b}^{1/2} \boldsymbol{H}_2(\boldsymbol{H}_1\boldsymbol{U} + \boldsymbol{G}_1\boldsymbol{V})^* \boldsymbol{G}_3\boldsymbol{X}$ at Bob at frequency f_3 with respect to the noise power of $\boldsymbol{N}_{3b}$ is denoted as SNR_3^{RDA},
$$SNR_3^{RDA} = \frac{q_{1b}q_{2b}q_{3b}}{\sigma_n^2} \quad (26)$$
It is assumed that $q_{3a} = q_{3b}$.
Here it needs to be pointed out that the SNR_3^{RDA} is greater than the SNR within the waveform $\boldsymbol{K}_b$ in (8) in terms of secret key extraction, since the noise introduced at frequencies f_1 and f_2, i.e., $\boldsymbol{N}_{1b}$ and $\boldsymbol{N}_{2b}$, are not involved in the definition of SNR_3^{RDA}.

The correlation coefficients $\rho^{RDA}_{\boldsymbol{K}_a\boldsymbol{K}_b}$ between the observed $\boldsymbol{K}_a$ and $\boldsymbol{K}_b$ in the proposed RDA assisted key generation systems are calculated for various SNR_x^{RDA} $(x = 1, 2, 3)$ scenarios, and are also depicted in Fig. 3. As expected, along with more

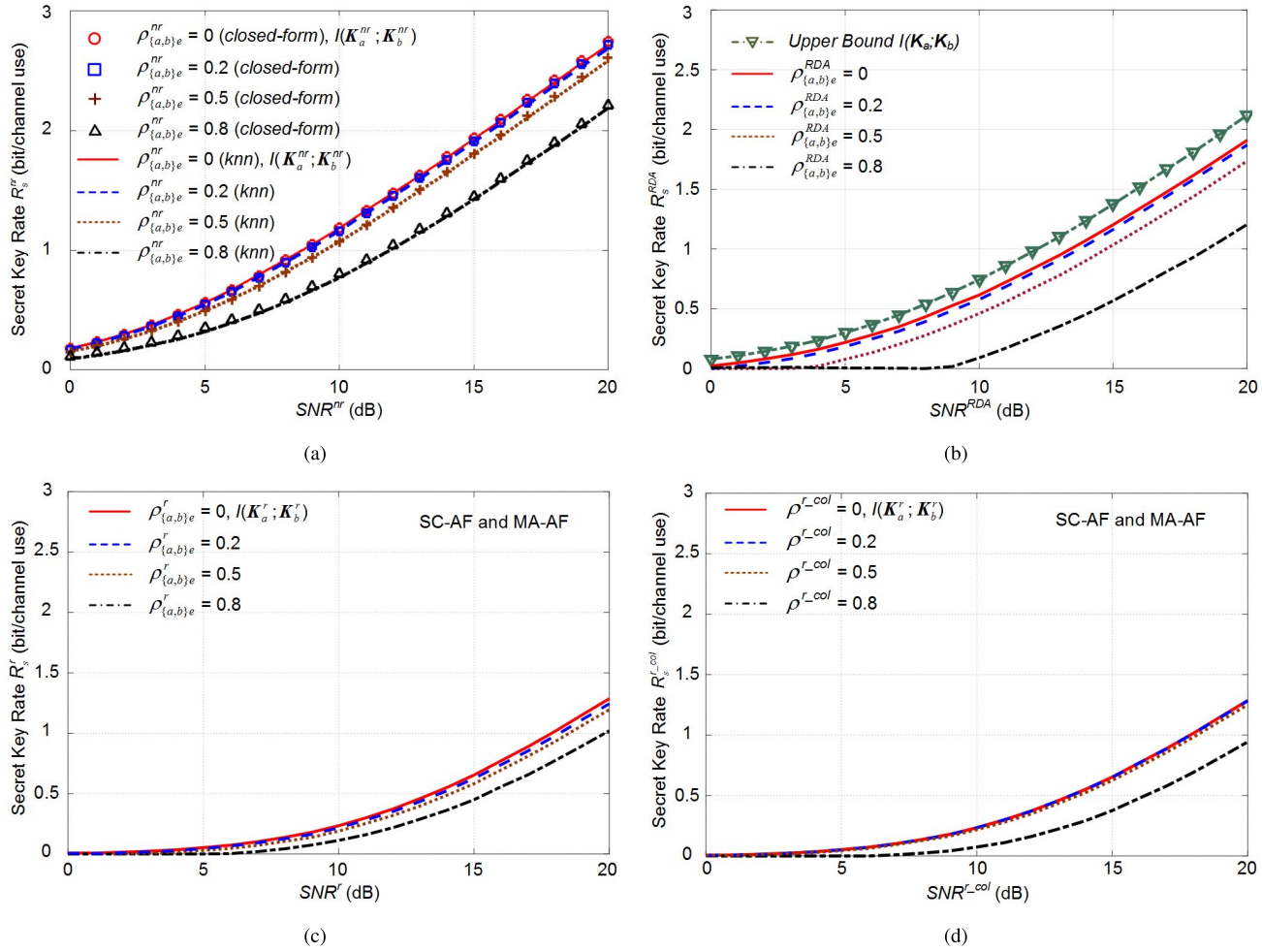


Fig. 4. Calculated secret key rates (a) R_s^{nr} (b) R_s^{RDA} (c) R_s^{r} (d) $R_s^{r\_col}$ in (a) non-relay (b) RDA assisted (c)(d) SC-AF and MA-AF key generation systems as functions of (a) SNR^{nr} (b) SNR^{RDA} (c) SNR^{r} (d) SNR^{r_col} when Eve's (Eves') antenna(s) is (are) placed close to Alice or (and) Bob.

key generation procedures, more noise is introduced into the waveforms shared between Alice and Bob, leading to reduced key correlation coefficients compared with that in the non-relay key generation system. However, a) as can be seen in Fig. 3, the performance degradation can be traded by configuring SNR_x^{RDA} through different key generation procedures; b) multiple key generation rounds can be conducted within a single channel coherence time period, since $\boldsymbol{U}_i$ and $\boldsymbol{V}_i$ can be randomly generated, leading to a greatly enhanced KGR. In order to facilitate discussion only the case of $SNR_{\{1,2,3\}}^{RDA} = SNR^{RDA}$ is investigated in the rest of the simulations in this paper.

The secret key rates in the non-relay key generation system, R_s^{nr}, when considering Eve's antenna being placed close to Alice or Bob, can be calculated using (11) by replacing $\boldsymbol{K}_{\{a,b,e\}}$ with their corresponding $\boldsymbol{K}_{\{a,b,e\}}^{nr}$. $\boldsymbol{K}_e^{nr}$ is the waveform obtained at Eve node used for secret key estimation in the non-relay key generation system. The term $I\left(Re(\boldsymbol{K}_a^{nr});\, Re(\boldsymbol{K}_b^{nr})\right)$ can be computed directly with the closed-form formula in (27), [54].

$$I\left(Re(\boldsymbol{K}_a^{nr});\, Re(\boldsymbol{K}_b^{nr})\right) = -\frac{1}{2}\log\left(1-\left(\rho^{nr}_{\boldsymbol{K}_a\boldsymbol{K}_b}\right)^2\right) \tag{27}$$

By obtaining correlation coefficients $\rho^{nr}_{\boldsymbol{K}_{\{a,b\}}\boldsymbol{K}_e}$ between $\boldsymbol{K}_{\{a,b\}}^{nr}$ and $\boldsymbol{K}_e^{nr}$ for different SNR^{nr}, the term $I\left(Re(\boldsymbol{K}_{\{a,b\}}^{nr});\, Re(\boldsymbol{K}_e^{nr})\right)$ can be computed similarly as in (27).

The calculated secret key rates R_s^{nr} in the non-relay key generation systems with different $\rho^{nr}_{\{a,b\}e}$ are depicted as a function of SNR^{nr} in Fig. 4(a). $\rho^{nr}_{\{a,b\}e}$ is the correlation coefficient between $\boldsymbol{H}^{nr}$ and the eavesdropping channels. Thus it is different to $\rho^{nr}_{\boldsymbol{K}_{\{a,b\}}\boldsymbol{K}_e}$, which can be computed from $\rho^{nr}_{\{a,b\}e}$ by using (28). The 'channel use' in Fig. 4 means a single key generation round.

$$\rho^{nr}_{\boldsymbol{K}_{\{a,b\}}\boldsymbol{K}_e} = \frac{SNR^{nr}}{SNR^{nr}+1}\rho^{nr}_{\{a,b\}e} \tag{28}$$

It should be noted that the closed-form formula in (27) is only applicable when the statistical distributions of observed waveforms are Gaussian, which does not necessarily hold in most other key generation systems, including the previous relay and our proposed RDA assisted key generation systems. Thus the results estimated using a mutual information calculation method that is based on k-nearest neighbor (knn) distances [55] are also presented and are shown good

agreement with the closed-form results, seen in Fig. 4(a). For system simulation results presented later in this paper, this *knn* distances method is adopted.

The secret key rates R_s^{RDA} in the proposed RDA assisted key generation systems are also calculated and shown in Fig. 4(b) for the same eavesdropping scenarios, i.e., Eve's antenna is placed close to Alice or Bob. Different from the non-relay case shown in Fig. 4(a), the RDA assisted key generation system is more susceptible in this eavesdropping scenario. It is also noticed that even when $\rho_{\{a,b\}e}^{RDA} = 0$, there is still an amount of information about the observed waveforms at the legitimate nodes leaked (The curve for $\rho_{\{a,b\}e}^{RDA} = 0$ is below the curve for the upper bound $I(\boldsymbol{K}_a; \boldsymbol{K}_b)$). This is due to the fact that the legitimate waveforms and intercepted waveforms take forms of $\boldsymbol{H}_2\boldsymbol{W}_{\{a,b\}}^*\boldsymbol{G}_3$ and $\boldsymbol{P}_2\boldsymbol{W}_a^*\boldsymbol{G}_3$ (or $\boldsymbol{H}_2\boldsymbol{W}_b^*\boldsymbol{Q}_3$). They are not independent even if $\boldsymbol{H}_2$ ($\boldsymbol{G}_3$) and $\boldsymbol{P}_2$ ($\boldsymbol{Q}_3$) are independent.

In Section VI, we will show that when equipping multiple antennas at the RDA node, the wireless transmission gains from the RDA towards the legitimate nodes, Alice or Bob, can be greater than those gains towards Eve, increasing R_s^{RDA} under the same $\rho_{\{a,b\}e}^{RDA}$ scenarios.

B. Comparison With Previous Relay Key Generation Systems in [35]

There have been a number of key generation methods reported, such as multi-antenna [24], multi-carrier [28], random beamforming [31], and relay based schemes [35]. The proposed RDA assisted key generation scheme in this paper is not a replacement of the multi-antenna, multi-carrier, and random beamforming schemes. In fact all of these techniques can be combined to lead to a further enhanced KGR. The combination can be straight-forward. Thus in our view it is not meaningful to compare the proposed RDA key generation system with these three types of schemes. However, since the proposed RDA key generation system is a relay-based scheme, the comparison with previous relay key generation systems is necessary, in order to claim the better performance that can be achieved in the proposed RDA key generation system. There have been several relay key generation systems reported, such as [17] and [33]–[37]. Among all previous reported relay key generation systems, we reckon that [35] investigated the most general relay key generation schemes, which, as a consequence, is selected to compare with the proposed RDA key generation system in this paper.

In [35] four relay key generation schemes were presented, which are classified by the authors as amplify-and-forward (AF), signal-combining amplify-and-forward (SC-AF), multiple-access amplify-and-forward (MA-AF), and amplify-and-forward with artificial noise (AF-AN). The AF scheme, as the authors pointed out, is not secure when the relay is monitored by Eve. The AF-AN scheme relies on the design of the artificial noise that is projected by the relay node towards Eve, but not Alice and Bob. For the architecture proposed in this paper, the generation of artificial noise using RDA for the benefit of wireless key generations will be presented separately in the future. Compared with the SC-AF, the MA-AF reduces the number of required time slots for a single key generation round from four to three at the cost of requirement for synchronization between Alice and Bob. The secret key rates in the SC-AF and MA-AF systems are almost identical when the unit 'bit/channel use' is adopted. They are both denoted as R_s^r in this paper.

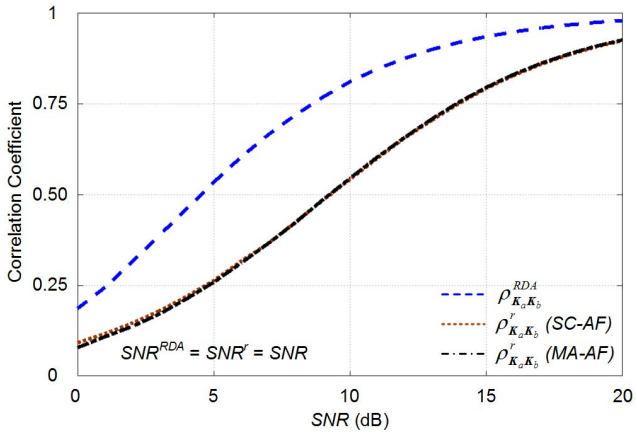


Fig. 5. Calculated correlation coefficients between observed waveforms at Alice and Bob used for secret key extraction in SC-AF, MA-AF, and proposed RDA assisted key generation systems.

In order to facilitate discussion in this paper, the waveforms acquired at Alice and Bob used for key generation purpose in the SC-AF scheme are presented in (29) and (30).

$$\boldsymbol{K}_a^r = \frac{1}{\sqrt{2}}\left[q_{r1}^{1/2}(\boldsymbol{H}^r + \boldsymbol{G}^r) + \boldsymbol{N}_{a2}^r + \boldsymbol{N}_{b2}^r\right]\boldsymbol{H}^r + \boldsymbol{N}_{a3}^r - \left(q_{r1}^{1/4}\boldsymbol{H}^r + \frac{\boldsymbol{N}_{a1}^r}{q_{r1}^{1/4}}\right)^2 \tag{29}$$

$$\boldsymbol{K}_b^r = \frac{1}{\sqrt{2}}\left[q_{r1}^{1/2}(\boldsymbol{H}^r + \boldsymbol{G}^r) + \boldsymbol{N}_{a2}^r + \boldsymbol{N}_{b2}^r\right]\boldsymbol{G}^r + \boldsymbol{N}_{b3}^r - \left(q_{r1}^{1/4}\boldsymbol{G}^r + \frac{\boldsymbol{N}_{b1}^r}{q_{r1}^{1/4}}\right)^2 \tag{30}$$

$\boldsymbol{H}^r$ ($\boldsymbol{G}^r$) refers to the Rayleigh wireless channel between Alice (Bob) and the relay. They are independent, and are normalized to be $E\left[|\boldsymbol{H}^r|^2\right] = E\left[|\boldsymbol{G}^r|^2\right] = 1$. It is assumed that all of the noise terms $\boldsymbol{N}_{\{a,b\}\{1,2,3\}}^r$ are independent and follow $CN(0, \sigma_r^2)$. The SNRs of signal transmissions in each step in the SC-AF key generation process are set to be identical, denoted as $SNR^r = q_{r1}/\sigma_r^2$.

In Fig. 5 the calculated correlation coefficients $\rho_{\boldsymbol{K}_a\boldsymbol{K}_b}^r$ between $\boldsymbol{K}_a^r$ and $\boldsymbol{K}_b^r$ in SC-AF and MA-AF schemes are presented and compared with its counterpart in the RDA assisted key generation systems. Clearly, it can be concluded that more noise involved in the SC-AF (MA-AF) key generation systems, seen in (29) and (30), reduces the achieved $\rho_{\boldsymbol{K}_a\boldsymbol{K}_b}^r$ significantly, when the channel SNRs are identical. The reduced $\rho_{\boldsymbol{K}_a\boldsymbol{K}_b}^r$ results in lower secret key rates R_s^r that are depicted in Fig. 4(c). The R_s^r is defined the same as R_s^{RDA} in (11) with $\boldsymbol{K}_{\{a,b,e\}}$ being replaced with their counterparts $\boldsymbol{K}_{\{a,b,e\}}^r$. Here $\boldsymbol{K}_e^r$, used for R_s^r calculation in Fig. 4(c), is the detected waveform by Eve which is placed close to Alice

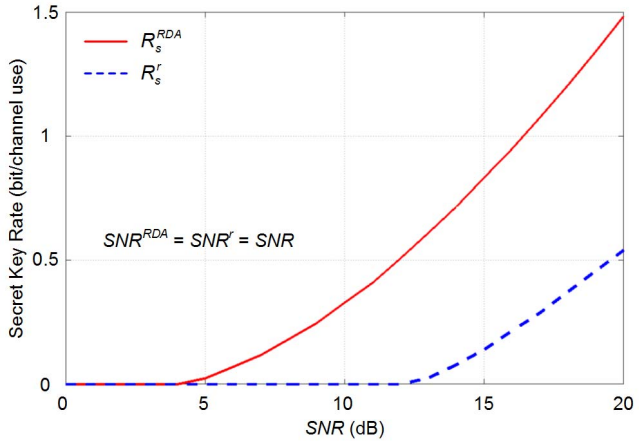


Fig. 6. Calculated secret key rates R_s^{RDA} and R_s^r in RDA and SC-AF (MA-AF) key generation systems as functions of SNR when Eve monitors the relay node.

or Bob. In this case, a pair of legitimate and eavesdropping channels with correlation coefficient $\rho^r_{\{a,b\}e}$ is created. The noise terms $\left(q_{r1}^{1/4}\{\boldsymbol{H}^r, \boldsymbol{G}^r\} + \boldsymbol{N}^r_{\{a,b\}1} \Big/ q_{r1}^{1/4}\right)^2$ in (29) and (30), on the other hand, reduce the amount of leaked information when Eve's antenna is placed close to Alice or Bob.

When Eve has the capability to intercept signals radiated by the relay node, the secret key rates, R_s^{RDA} and R_s^r are obtained and compared in Fig. 6. During the calculation it is found that in the RDA key generation system, using $\boldsymbol{K}_e^{\mathbf{TS}1}\boldsymbol{K}_e^{\mathbf{TS}2}$ as $\boldsymbol{K}_{\{a,b\}}$ estimation at Eve node is always better than using individual $\boldsymbol{K}_e^{\mathbf{TS}\{1,2\}}$. For R_s^r calculation in the SC-AF and MA-AF systems the waveforms used for secret key estimation at Eve node are designed as

$$\boldsymbol{K}_e^r = \tfrac{1}{2}\left[q_{r1}^{1/2}(\boldsymbol{H}^r + \boldsymbol{G}^r) + \boldsymbol{N}^r_{a2} + \boldsymbol{N}^r_{b2}\right]^2, \tag{31}$$

as adopted in [35].

In order to facilitate comparison with the proposed RDA key generation scheme, the same eavesdropping strategy of colluding Eves for SC-AF and MA-AF is now investigated, which were not studied in [35]. From (29) and (30) it can be seen that the common waveform that is used for key extraction at Alice and Bob nodes is $\frac{1}{\sqrt{2}}q_{r1}^{1/2}\boldsymbol{H}^r\boldsymbol{G}^r$. Hence, with the colluding capability different Eves can separately estimate $\boldsymbol{H}^r$ and $\boldsymbol{G}^r$, respectively, and then combine them to construct $\boldsymbol{K}_e^{r\_col}$, see (32), (33), and (34).

$$\boldsymbol{K}_e^{r\_col} = \frac{1}{\sqrt{2}}q_{r1}^{1/2}\hat{\boldsymbol{H}}^r\hat{\boldsymbol{G}}^r \tag{32}$$

$$q_{r1}^{1/2}\hat{\boldsymbol{H}}^r = q_{r1}^{1/2}\boldsymbol{P}^r + \boldsymbol{N}^r_{e1} \tag{33}$$

$$q_{r1}^{1/2}\hat{\boldsymbol{G}}^r = q_{r1}^{1/2}\boldsymbol{Q}^r + \boldsymbol{N}^r_{e2} \tag{34}$$

Here two pairs of correlating channels $\boldsymbol{H}^r$ (or $\boldsymbol{G}^r$) and $\boldsymbol{P}^r$ (or $\boldsymbol{Q}^r$) with correlation coefficient $\rho^r_{\boldsymbol{HP}}$ ($\rho^r_{\boldsymbol{GQ}}$) are created. $\boldsymbol{P}^r$ ($\boldsymbol{Q}^r$) is the channel coefficient between the relay and the Eve whose antenna is placed close to Alice (Bob) in time slot 1 in both SC-AF and MA-AF schemes, see [35, Fig. 2]. The noise terms $\boldsymbol{N}^r_{e\{1,2\}}$ are independent, and are assumed to follow the same distribution as $\boldsymbol{N}^r_{\{a,b\}1}$, i.e., $\boldsymbol{N}^r_{e\{1,2\}} \sim CN(0, \sigma_r^2)$. Similarly, SNR^{r_col} is defined as q_{r1}/σ_r^2. In Fig. 4(d) the calculated system secret rates $R_s^{r\_col}$ are presented for various ρ^{r_col}, here $\rho^{r\_col} = \rho^r_{\boldsymbol{HP}} = \rho^r_{\boldsymbol{GQ}}$. Compared with those in Fig.4(c), it can be seen that only when the legitimate channels and eavesdropping channels are highly correlated, collaboratively estimating each factor within the shared waveforms between Alice and Bob in SC-AF (MA-AF) scheme helps interception of secret keys.

From Figs. 4(b), 4(c), 4(d), and 6 it can be concluded that the proposed RDA assisted key generation system outperforms, with regard to secrecy performance, both the previous SC-AF and MA-AF relay key generation systems in [35].

Table I summarizes the characteristics of the non-relay, the SC-AF, the MA-AF, and the proposed RDA assisted wireless key generation systems. From Fig. 4(b) it can seen that the proposed RDA assisted wireless key generation system is relatively sensitive to the eavesdropping when Eve's antenna is placed close to Alice or Bob. This vulnerability can be alleviated by exploiting more antenna elements in the RDA which is investigated in Section VI.

V. Impact of Imperfect Training Sequence on System Performance

When the training sequence $\boldsymbol{X}$ is not perfectly shared among all nodes in advance, it has to be distributed via actual wireless transmissions during the key generation process. In this section the impact of this wireless distributed and recovered $\boldsymbol{X}$ on the system performance is investigated.

In **TS**1 Alice transmits training $\boldsymbol{X}$ at frequency f_2, which can be detected by Bob as

$$\hat{\boldsymbol{X}}_b = q_{2b}^{1/2}\boldsymbol{H}_{ab}\boldsymbol{X} + \boldsymbol{N}^{ab}_{2b}, \tag{35}$$

where $\boldsymbol{H}_{ab}$ is the wireless channel between Alice and Bob at frequency f_2, and $\boldsymbol{N}^{ab}_{2b}$ is the independent AWGN $\sim CN(0, \sigma_b^2)$. In the meantime, when the Eve antenna is placed close to Bob, an estimation of $\boldsymbol{X}$ can be obtained by Eve as

$$\hat{\boldsymbol{X}}_e = q_{2b}^{1/2}\boldsymbol{H}_{ae}\boldsymbol{X} + \boldsymbol{N}^{ae}_{2e}. \tag{36}$$

Here $\boldsymbol{H}_{ae}$ and $\boldsymbol{N}^{ae}_{2e}$ are defined the same as $\boldsymbol{H}_{ab}$ and $\boldsymbol{N}^{ab}_{2b}$, but they are associated with Eve instead. $\boldsymbol{N}^{ae}_{2e} \sim CN(0, \sigma_e^2)$, and it is assumed that $\sigma_e = \sigma_b$.

Similarly in **TS**2, Bob transmits training $\boldsymbol{Z}$ at frequency f_3, which can be recovered at Alice and Eve positioned close to Alice, respectively. The training sequence $\boldsymbol{Z}$ used by Bob is different to the $\boldsymbol{X}$ used by Alice. The estimations of $\boldsymbol{Z}$ at Alice and Eve nodes are denoted in

$$\hat{\boldsymbol{Z}}_a = q_{3a}^{1/2}\boldsymbol{G}_{ba}\boldsymbol{Z} + \boldsymbol{N}^{ba}_{3a}, \tag{37}$$

and

$$\hat{\boldsymbol{Z}}_e = q_{3a}^{1/2}\boldsymbol{G}_{be}\boldsymbol{Z} + \boldsymbol{N}^{be}_{3e}. \tag{38}$$

$\boldsymbol{G}_{ba}$ (or $\boldsymbol{G}_{be}$) is the wireless channel coefficient between Bob and Alice (or Eve positioned close to Alice) at frequency f_3. The noise terms $\boldsymbol{N}^{ba}_{3q}$ and $\boldsymbol{N}^{be}_{3e}$ are assumed to have the same distribution with $\boldsymbol{N}^{ab}_{2b}$ and $\boldsymbol{N}^{ae}_{2e}$.

TABLE I
SUMMARY OF CHARACTERISTICS OF NON-RELAY, SC-AF, MA-AF, AND PROPOSED RDA ASSISTED KEY GENERATION SYSTEMS

	Non-relay	SC-AF	MA-AF	RDA
Number of required time slots	2	4	3	2
Nodes requiring knowledge for time slots	Alice and Bob	Alice, Bob, and relay	Alice, Bob, and relay	Alice and Bob
Strict time synchronization	No	No	Yes	No
Requirement for calculation capability in the relay node	Not applicable	Yes	Yes	No
Correlation coefficient between waveform observations at Alice and Bob	High (Fig. 3)	Low (Fig. 5)	Low (Fig. 5)	Medium (Fig. 3)
R_s when Eve's antenna is placed close to Alice and/or Bob	High and insensitive (Fig. 4(a))	Low but insensitive (Fig. 4(c), Fig. 4(d))	Low but insensitive (Fig. 4(c), Fig. 4(d))	Medium but sensitive (Fig. 4(b))
R_s when Eve is able to intercept signals transmitted by the relay	Not applicable	Low (Fig. 6)	Low (Fig. 6)	Medium (Fig. 6)
Multiple key generation rounds within one T_c	No	No	No	Yes

Since it is assumed that Eve is placed either close to Bob in **TS**1 or close to Alice in **TS**2, it is reasonable to set the magnitudes of legitimate and eavesdropping channel pair to be identical, i.e., $E\left(|\boldsymbol{H}_{ab}|^2\right) = E\left(|\boldsymbol{H}_{ae}|^2\right)$ and $E\left(|\boldsymbol{G}_{ba}|^2\right) = E\left(|\boldsymbol{G}_{be}|^2\right)$. Under these conditions, the SNRs in the training stage can be defined in (39) and (40).

$$SNR_{t1} = \frac{q_{2b}E\left(|\boldsymbol{H}_{a\{b,e\}}|^2\right)}{\sigma^2_{\{b,e\}}} \tag{39}$$

$$SNR_{t2} = \frac{q_{3a}E\left(|\boldsymbol{G}_{b\{a,e\}}|^2\right)}{\sigma^2_{\{b,e\}}} \tag{40}$$

With the imperfectly recovered training sequences, the waveform observations obtained by Bob and Alice for secret key extractions in (8) and (10), respectively, are thus contaminated, and they are expressed in (41) and (42).

$$\boldsymbol{K}_b{}' = \frac{1}{k_1\hat{\boldsymbol{X}}_b}\left(q_{3b}^{1/2}q_{2b}^{1/2}\boldsymbol{G}_3\boldsymbol{W}_b^*\boldsymbol{H}_2\boldsymbol{X} + q_{3b}^{1/2}\boldsymbol{G}_3\boldsymbol{W}_b^*\boldsymbol{N}_{2b} + \boldsymbol{N}_{3b}\right) \tag{41}$$

$$\boldsymbol{K}_a{}' = \frac{1}{k_2\hat{\boldsymbol{Z}}_a}\left(q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_a^*\boldsymbol{G}_3\boldsymbol{Z} + q_{2a}^{1/2}\boldsymbol{H}_2\boldsymbol{W}_a^*\boldsymbol{N}_{3a} + \boldsymbol{N}_{2a}\right) \tag{42}$$

Similarly the intercepted waveforms by Eves that are placed close to Bob or Alice can be written as

$$\boldsymbol{K}_e^{be\prime} = \frac{1}{k_1\hat{\boldsymbol{X}}_e}\left(q_{3b}^{1/2}q_{2b}^{1/2}\boldsymbol{Q}_3\boldsymbol{W}_b^*\boldsymbol{H}_2\boldsymbol{X} + q_{3b}^{1/2}\boldsymbol{Q}_3\boldsymbol{W}_b^*\boldsymbol{N}_{2b} + \boldsymbol{N}_{3e}^{be}\right), \tag{43}$$

and

$$\boldsymbol{K}_e^{ae\prime} = \frac{1}{k_2\hat{\boldsymbol{Z}}_e}\left(q_{2a}^{1/2}q_{3a}^{1/2}\boldsymbol{P}_2\boldsymbol{W}_a^*\boldsymbol{G}_3\boldsymbol{Z} + q_{2a}^{1/2}\boldsymbol{P}_2\boldsymbol{W}_a^*\boldsymbol{N}_{3a} + \boldsymbol{N}_{2e}^{ae}\right). \tag{44}$$

The coefficients k_1 and k_2 are added for power normalization and they equal to $q_{2b}\sqrt{E\left(|\boldsymbol{H}_{a\{b,e\}}|^2\right)}$ and $q_{3a}\sqrt{E\left(|\boldsymbol{G}_{b\{a,e\}}|^2\right)}$, respectively.

Using (41), (42), (43), and (44), the secret key rates in the proposed RDA assisted key generation system were calculated for the case when Eve's antenna is placed close to Alice or Bob ($\rho^{RDA}_{\{a,b\}e} = 0.5$) and imperfect training sequence recovery is assumed. The results are illustrated in Fig. 7. As can be expected, the higher quality of the wireless channel for training sequence transmission, i.e., higher SNR_{t1} and SNR_{t2}, makes the secrecy performance of the system converge to that of the system with perfectly shared training sequence. It is also worth mentioning that an SNR_t of only 15 dB is sufficient to maintain the performance advantage over that can be achieved in the previous relay key generation systems even with the assumption of perfect training sequence recovery, see Fig. 4(c) for comparison.

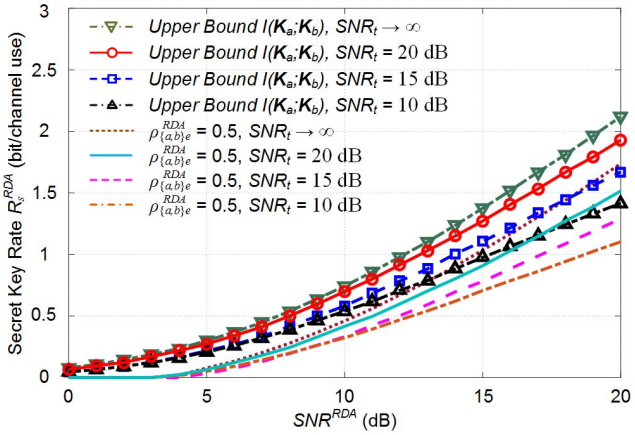


Fig. 7. Calculated secret key rates R_s^{RDA} in the proposed RDA assisted key generation systems as functions of SNR^{RDA} and SNR_t when Eve's antenna is placed close to Alice or Bob. $\rho^{RDA}_{\{a,b\}e} = 0.5$ and $SNR_t = SNR_{t1} = SNR_{t2}$.

VI. MULTI-ANTENNA RDA ASSISTED KEY GENERATION

In this section the benefit of using multiple RDA antenna elements in the proposed key generation architecture is investigated. We do not exploit multiple wireless propagation channels between Alice (or Bob) and each antenna in the RDA to extract more secret keys in one key generation round.

This is because in order to separate multiple propagation channels more time slots are required and the RDA has to know time slot assignment. And more importantly, when using 'bit/time slot' as the unit the achievable secret key rates do not increase with the number M of the antenna elements in the RDA. Instead we investigate the beamforming gains that multiple RDA antenna elements can bring for the improvement of the system secrecy performance under the scenario that Eve's antenna is placed close to Alice or Bob.

The response of a multipath wireless channel is a function of both frequency and time. As we discussed in Section II, when compared with the channel coherence time T_c in a typical in-door multipath environment which is normally in the order of tens to hundreds of ms, the RDA operation, i.e., signal reception, phase conjugation, and re-transmission, occurs within hundreds of μs, and thus it can be regarded as 'real-time', i.e., the channel response is constant with respect to time during RDA operation. As a consequence only the frequency configuration of an RDA is investigated. In order to enable RDA phase conjugation operation a pilot signal, e.g., $\boldsymbol{U}$ and $\boldsymbol{V}$ used in the proposed scheme, normally needs to be constantly present. For the purpose of increasing isolation between the received pilot signal and the re-transmitted signal, frequency-division duplexing for signal reception and signal re-transmission is commonly adopted [38], [46].

In the proposed key generation architecture in this paper, the RDA node receives the pilot signals at frequency f_1 and re-transmits signals at frequency f_3 in **TS**1 and at frequency f_2 in **TS**2. As we discussed in Section II.B in a multipath environment when the phase conjugation frequency is different from the signal re-transmission frequency, (5) does not hold. This means re-transmitted common signals by each RDA antenna cannot be combined in-phase at the location where the pilot signal is originated, resulting in reduced beamforming gains, compared with ideal beamforming gains. In following discussions only the transmission from the RDA to Bob in **TS**1 is considered. In this case the relative beamforming gain ΔG_b in dB, experienced at Bob node, is defined as

$$\Delta G_b = 10\log_{10}\left(\frac{E\left(\left|\vec{\boldsymbol{H}}_2 \circ \left(\vec{\boldsymbol{H}}_1\boldsymbol{U} + \vec{\boldsymbol{G}}_1\boldsymbol{V}\right)^* \cdot \vec{\boldsymbol{G}}_3\right|^2\right)}{E\left(\left|\vec{\boldsymbol{H}}_2 \circ \left(\vec{\boldsymbol{H}}_1\boldsymbol{U} + \vec{\boldsymbol{G}}_1\boldsymbol{V}\right)^* \cdot \vec{\boldsymbol{G}}_1\right|^2\right)}\right). \tag{45}$$

Here the ideal beamforming gain corresponds to the link gain between the RDA and Bob when the frequencies for pilot reception and signal re-transmission are identical, i.e., $f_1 = f_3$, so that $\vec{\boldsymbol{G}}_3$ becomes $\vec{\boldsymbol{G}}_1$. All of the vectors in (45) have M elements with the m^{th} entry representing the channel coefficients between Alice or Bob and the m^{th} RDA antenna element at the corresponding frequencies.

In order to facilitate discussion in this section it is assumed that the signal magnitudes radiated by each RDA antenna element are identical and channels between each RDA antenna and Bob are independent Rayleigh fading. The amount of the loss of beamforming gains is determined by the level of similarity between the channel involved in phase conjugation process, i.e., $\vec{\boldsymbol{G}}_1$, and the channel used for signal re-transmissions, i.e., $\vec{\boldsymbol{G}}_3$. The level of similarity, quantified as channel correlation coefficients r_{fb}, is a function of their frequency separation $\Delta f = f_3 - f_1$ and channel frequency characteristics described with parameter σ_τ. r_{fb} is calculated using (3) with $\boldsymbol{H}(f,t)$ and $\boldsymbol{H}(f+\Delta f, t+\Delta t)$ being replaced with $\vec{\boldsymbol{G}}_1$ and $\vec{\boldsymbol{G}}_3$, respectively.

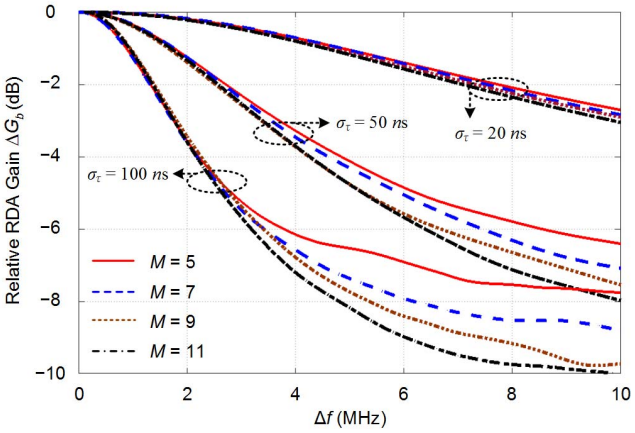


Fig. 8. Simulated relative RDA re-transmission gains ΔG_b for various σ_τ, Δf, and M.

In Fig. 8 the simulated relative RDA re-transmission beamforming gains, ΔG_b are illustrated for a range of frequency separations Δf, and also for different numbers M of RDA antenna elements. Multipath channels with σ_τ of 20 ns, 50 ns, and 100 ns are considered. Values of delay spread other than 20 ns, 50 ns, and 100 ns can be equivalently adopted. The results shown in Fig. 8 are averaged over 2000 time instants that are separated far beyond the channel coherence time T_c. As expected for a fixed RDA element M, greater frequency spacing Δf and RMS delay spread σ_τ lead to lower relative re-transmission beamforming gain. This is because in these cases the propagation channels $\vec{\boldsymbol{G}}_1$ and $\vec{\boldsymbol{G}}_3$, at signal reception and re-transmission frequencies respectively, are less correlated. Similarly, when the channel and frequency spacing are fixed, i.e., σ_τ and Δf are fixed, greater numbers of RDA elements result in lower relative RDA re-transmission beamforming gain. This can be explained that more array antenna elements generate radiation beam patterns with narrower main beams which are more susceptible to the dissimilarity between the wireless channels at frequencies f_1 and f_3, i.e., $\vec{\boldsymbol{G}}_1$ and $\vec{\boldsymbol{G}}_3$.

Since the channel correlation coefficient r_{fb} between $\vec{\boldsymbol{G}}_1$ and $\vec{\boldsymbol{G}}_3$ is a function of both σ_τ and Δf, the curves in Fig. 8 can be simplified by plotting relative RDA beamforming gains ΔG_b against r_{fb}, shown in Fig. 9. $r_{fb} = 1$ means that either the RDAs receive and re-transmit at the same frequency, i.e. $\Delta f = 0$, or the wireless channels are flat-fading, i.e., $L = 1$.

We deliberately write the axis units in Fig. 9 as r_f and ΔG, instead of r_{fb} and ΔG_b. This is because the Fig. 9 can also be applicable to r_{fe} and ΔG_e, when Eve's antenna is placed close to Bob. r_{fe} is the channel correlation coefficient between $\vec{\boldsymbol{G}}_1$ and the eavesdropping channel $\vec{\boldsymbol{Q}}_3$. It is noted that $\vec{\boldsymbol{G}}_1$ and $\vec{\boldsymbol{G}}_3$ is correlated with coefficient r_{fb}, and $\vec{\boldsymbol{G}}_3$ and $\vec{\boldsymbol{Q}}_3$

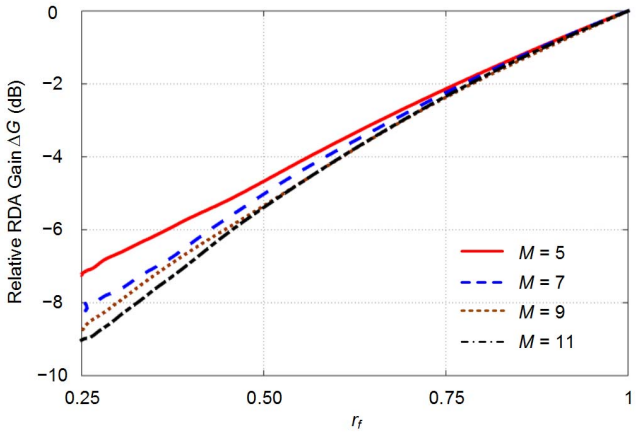


Fig. 9. Simulated relative RDA re-transmission gains as functions of channel correlation coefficients r_f for different number M of RDA elements.

TABLE II

SIMULATED EXAMPLE OF $r_{f\{b,e\}}$ AND $\Delta G_{\{b,e\}}$ FOR DIFFERENT NUMBERS M OF RDA ELEMENTS. ($\sigma_\tau = 50$ ns, $\Delta f = 2$ MHz, $\rho_{be}^{RDA} = 0.5$)

M	5	7	9	11
r_{fb}	0.862	0.860	0.859	0.858
r_{fe}	0.435	0.434	0.424	0.417
ΔG_b (dB)	−1.14	−1.24	−1.26	−1.29
ΔG_e (dB)	−5.37	−5.92	−6.41	−6.60
$\Delta G_b - \Delta G_e$ (dB)	4.23	4.68	5.15	5.31

TABLE III

SIMULATED EXAMPLE OF $r_{f\{b,e\}}$ AND $\Delta G_{\{b,e\}}$ FOR DIFFERENT NUMBERS M OF RDA ELEMENTS. ($\sigma_\tau = 50$ ns, $\Delta f = 2$ MHz, $\rho_{be}^{RDA} = 0.2$)

M	5	7	9	11
r_{fb}	0.862	0.860	0.859	0.858
r_{fe}	0.176	0.162	0.160	0.159
ΔG_b (dB)	−1.14	−1.24	−1.26	−1.29
ΔG_e (dB)	−7.80	−9.03	−9.73	−10.36
$\Delta G_b - \Delta G_e$ (dB)	6.66	7.79	8.47	9.07

is correlated with coefficient ρ_{be}^{RDA}. ΔG_e is defined similarly as in (45) with $\vec{G}_3$ being replaced with $\vec{Q}_3$.

Two examples of achieved relative RDA beamforming gains toward Bob and Eve, i.e., ΔG_b and ΔG_e, together with associated r_{fb} and r_{fe} are provided in Table II and Table III. The difference of ΔG_b and ΔG_e corresponds to the difference of received SNRs at Bob and Eve nodes when the added channel noise $\vec{N}_{3b}$ at Bob and $\vec{N}_{3e}^{be}$ at Eve have the same distribution. It is this gain difference $\Delta G_b - \Delta G_e$ that determines the amount of improvement of secrecy performance when multiple antennas at RDA node are employed. For better illustration the gain differences $\Delta G_b - \Delta G_e$ are plotted for various σ_τ, Δf, ρ_{be}^{RDA}, and M in Fig. 10. As can be concluded, the smaller values of σ_τ, Δf, and ρ_{be}^{RDA}, and the greater number M lead to larger gain differences $\Delta G_b - \Delta G_e$. Intuitively, when σ_τ and/or $\Delta f \to \infty$, the frequencies of receive and re-transmission at RDA node are

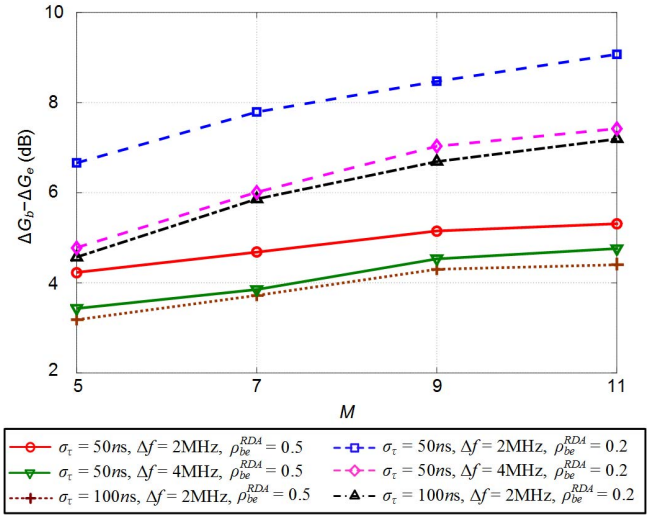


Fig. 10. Gain differences $\Delta G_b - \Delta G_e$ as a function of σ_τ, Δf, ρ_{be}^{RDA}, and M when EveâĽ™s antenna is placed close to Bob.

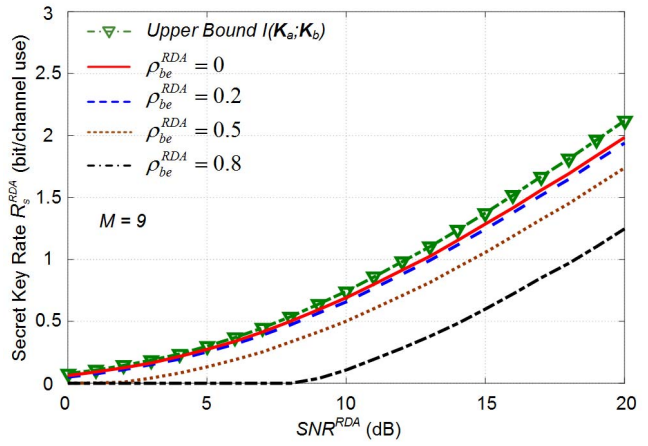


Fig. 11. Calculated secret key rates R_s^{RDA} in 9-element RDA assisted key generation systems as functions of SNR^{RDA} when EveâĽ™s antenna is placed close to Bob. ($\sigma_\tau = 50$ ns and $\Delta f = 2$ MHz).

separated far beyond the coherence bandwidth, resulting in no beamforming gain towards the legitimate keying nodes in the multi-antenna RDA scenario. The gain differences, namely, the differences of SNRs at Bob and Eve nodes, make the proposed RDA assisted key generation systems less vulnerable under the eavesdropping strategy of placing Eve's antenna close to Alice or Bob, especially for small $\rho_{\{a,b\}e}^{RDA}$. Fig. 11 gives an example of the simulated R_s^{RDA} for different ρ_{be}^{RDA}. In this example it is assumed that $\sigma_\tau = 50$ ns, $\Delta f = 2$ MHz, and $M = 9$. Compared with R_s^{RDA} shown in Fig. 4(b), it can be seen that more RDA antenna elements help reduce the chance of being intercepted by the Eve positioned around Alice or Bob. In addition greater beamforming gains enabled by adopting more RDA antennas reduce the transmitted power by the RDA under the same system SNR requirement.

VII. CONCLUSION

A new type of wireless key generation system architecture, using an RDA as a relay node, was proposed and analyzed in this paper. By configuring analogue RDAs receive

and re-transmit at different frequencies, the number of time slots required for each key generation round was reduced to two. Furthermore, the equivalent reciprocal wireless channels between legitimate keying nodes can be controlled, by Alice and Bob, to be 'fast fading', which is able to increase KGRs significantly. Also distinct from the previous relay based key generation systems, the RDAs employed do not need to have additional digital computational capability, and do not need to acquire knowledge about system parameters, such as time slots assignment and training sequences, which makes this architecture more flexible in terms of adding more legitimate keying nodes and/or more RDA relay nodes. Through simulations it was shown that the proposed RDA assisted key generation systems have better secrecy performance than that in the previous relay key generation systems, under various eavesdropping strategies.

REFERENCES

[1] A. Kahate, *Cryptography and Network Security*, 3rd ed. New Delhi, India: McGraw-Hill, 2013.

[2] A. Ja. (2015, Sep). "Will quantum computers threaten modern cryptography." [Online]. Available: http://www.tripwire.com/state-of-security/featured/will-quantum-computers-threaten-modern-cryptography

[3] A. S. K. Pathan, H.-W. Lee, and C. S. Hong, "Security in wireless sensor networks: Issues and challenges," in *Proc. 8th Int. Conf. Adv. Commun. Technol. (ICACT)*, vol. 2. Feb. 2006, pp. 1043–1048.

[4] L. Roselli *et al.*, "Smart surfaces: Large area electronics systems for Internet of Things enabled by energy harvesting," *Proc. IEEE*, vol. 102, no. 11, pp. 1723–1746, Nov. 2014.

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[6] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[7] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[8] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[9] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[10] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. Workshop Wireless Commun. Security Phys. Layer*, Coimbra, Portugal, Jul. 2015, pp. 267–272.

[11] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, vol. 2010, pp. 1–21, Jun. 2016.

[12] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Beijing, China, Sep. 2009, pp. 321–332.

[14] B. Zan, M. Gruteser, and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," in *Proc. Int. Conf. Comput. Netw. Commun.*, Maui, HI, USA, Jan./Feb. 2012, pp. 980–984.

[15] S. N. Premnath, J. Croft, N. Patwari, and S. K. Kasera, "Efficient high-rate secret key extraction in wireless sensor networks using collaboration," *ACM Trans. Sensor Netw.*, vol. 11, no. 1, 2014, Art. no. 2.

[16] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1422–1430.

[17] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[18] J.-J. Huang and T. Jiang, "Physical layer secret key generation scheme used in 60 GHz band," *J. China Univ. Posts Telecommun.*, vol. 21, no. 5, pp. 76–82, Nov. 2014.

[19] J. Huang and T. Jiang, "Secret key generation exploiting ultra-wideband indoor wireless channel characteristics," *Security Commun. Netw.*, vol. 8, no. 13, pp. 2329–2337, Sep. 2015.

[20] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[21] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[22] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. 17th IEEE Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Edinburgh, U.K., Jul. 2016, pp. 1–5.

[23] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag. (EuCAP)*, Berlin, Germany, Mar. 2009, pp. 1499–1503.

[24] K. Zeng, D. Wu, A. J. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, San Diego, CA, Mar. 2010, pp. 1–9.

[25] B. Zan and M. Gruteser, "Random channel hopping schemes for key agreement in wireless networks," in *Proc. IEEE PIMRC*, Tokyo, Japan, Sep. 2009, pp. 2886–2890.

[26] L. Yao, S. T. Ali, V. Sivaraman, and D. Ostry, "Decorrelating secret bit extraction via channel hopping in body area networks," in *Proc. IEEE PIMRC*, Sydney, Australia, Sep. 2012, pp. 1454–1459.

[27] G. Revadigar, C. Javali, H. J. Asghar, K. B. Rasmussen, and S. Jha, "Mobility independent secret key generation for wearable healthcare devices," in *Proc. BodyNets*, Sydney, Australia, Sep. 2015, pp. 294–300.

[28] S. Yasukawa, H. Iwai, and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM," in *Proc. Int. Symp. Inf. Theory Appl.*, Auckland, New Zealand, Dec. 2008, pp. 1–6.

[29] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.

[30] J. Zhang *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[31] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2292–2300.

[32] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1278–1287, Aug. 2012.

[33] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[34] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov. 2013.

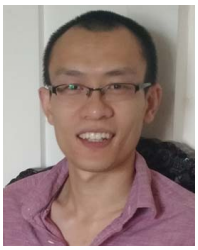
[35] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[36] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[37] C. Javali, G. Revadigar, M. Ding, and S. Jha, "Secret key generation by virtual link estimation," in *Proc. ACM BodyNets*, Sydney, Australia, Sep. 2015, pp. 301–307.

[38] V. Fusco and N. Buchanan, "Developments in retrodirective array technology," *Microw., Antennas Propag., IET*, vol. 7, no. 2, pp. 131–140, Jan. 2013.

[39] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.
[40] V. Erceg *et al.*, *TGn Channel Models*, IEEE Standard 802.11-03/940r4, May 2004.
[41] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul. 1998.
[42] S. Bernard, *Digital Communications Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2001.
[43] P. Chan and V. Fusco, "Bi-static 5.8GHz RFID range enhancement using retrodirective techniques," in *Proc. 41st Eur. Microw. Conf. (EuMC)*, Manchester, U.K., Oct. 2011, pp. 976–979.
[44] P. V. Brennan, "An experimental and theoretical study of self-phased arrays in mobile satellite communications," *IEEE Trans. Antennas Propag.*, vol. 37, no. 11, pp. 1370–1376, Nov. 1989.
[45] N. B. Buchanan, V. F. Fusco, and M. van der Vorst, "Satcom retrodirective array," *IEEE Trans. Microw. Theory Techn.*, vol. 64, no. 5, pp. 1614–1621, May 2016.
[46] L. Chen, Y. C. Guo, X. W. Shi, and T. L. Zhang, "Overview on the phase conjugation techniques of the retrodirective array," *Int. J. Antennas Propag.*, vol. 2010, Apr. 2010, Art. no. 564357.
[47] V. Fusco, C. B. Soo, and N. Buchanan, "Analysis and characterization of PLL-based retrodirective array," *IEEE Trans. Microw. Theory Techn.*, vol. 53, no. 2, pp. 730–738, Feb. 2005.
[48] N. Buchanan, V. Fusco, and M. van der Vorst, "New retrodirective antenna techniques for mobile terminal applications," in *Proc. 32nd Antenna Workshop, ESA/ESTEC*, Noordwijk, The Netherlands, Oct. 2010, pp. 5–8.
[49] N. B. Buchanan and V. F. Fusco, "Modulation insensitive PLL for tracking antenna applications," *Microw. Opt. Technol. Lett.*, vol. 57, no. 6, pp. 1286–1289, Jun. 2015.
[50] N. B. Buchanan, V. Fusco, and M. van der Vorst, "Phase conjugating circuit with frequency offset beam pointing error correction facility for precision retrodirective antenna applications," in *Proc. 41st Eur. Microw. Conf. (EuMC)*, Manchester, U.K., Oct. 2011, pp. 1281–1283.
[51] Y. Ding and V. Fusco, "Improved physical layer secure wireless communications using a directional modulation enhanced retrodirective array," in *Proc. XXXIth URSI General Assembly Sci. Symp. (URSI GASS)*, Beijing, China, Aug. 2014, pp. 1–4.
[52] K. Chen and B. B. Natarajan, "Mimo-based secret key generation strategies: Rate analysis," *Int. J. Mobile Comput. Multimedia Commun.*, vol. 6, no. 3, pp. 22–55, Jan. 2015.
[53] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," *Phys. Commun.*, vol. 19, pp. 1–10, Jun. 2016.
[54] J. A. Thomas and T. Cover, *Elements of Information Theory*, 2nd ed. New York, NJ, USA: Wiley, 2006.
[55] A. Kraskov and H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, no. 6, p. 066138, Jun. 2004.



Yuan Ding received the bachelor's degree from Beihang University, Beijing, China, in 2004, the master's degree from Tsinghua University, Beijing, in 2007, and the Ph.D. degree from the Queen's University of Belfast, Belfast, U.K., in 2014, all in electronic engineering.

He was a Radio Frequency (RF) Engineer with the Motorola Research and Development Centre, Beijing, China, from 2007 to 2009, and was an RF Field Application Engineer, responsible for high power base-station amplifier design with Freescale Semiconductor Inc., Beijing, China, from 2009 to 2011. He is currently a Research Fellow with the ECIT Institute, Queen's University of Belfast, Belfast, U.K. His research interests are in antenna array, physical layer security, and 5G related areas.

Dr. Ding was a recipient of the IET Best Student Paper Award at LAPC 2013 and a recipient of the Young Scientists Awards in General Assembly and Scientific Symposium, 2014 31st URSI.

Junqing Zhang received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China, in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from the Queen's University of Belfast, U.K., in 2016. He is currently a Post-Doctoral Research Fellow with the Queen's University of Belfast. His current research interests include physical layer security, cryptography, and OFDM.

Vincent F. Fusco (S'82–M'82–SM'96–F'04) received the bachelor's degree (Hons.) in electrical and electronic engineering, the Ph.D. degree in microwave electronics, and the D.Sc. degree from the Queen's University of Belfast (QUB), Belfast, U.K., in 1979, 1982, and 2000, respectively.

His work was focused on advanced front-end architectures with enhanced functionality. He is the Chief Technology Officer of ECIT, QUB. He has authored over 450 scientific papers in major journals and in refereed international conferences. He has authored two textbooks, holds patents related to self-tracking antennas, and has contributed invited papers and book chapters. His current research interests include active antenna and front-end MMIC techniques.

Dr. Fusco is a fellow of the Institution of Engineering and Technology, the Royal Academy of Engineers, and the Royal Irish Academy. In 2012, he received the IET Senior Achievement Award and the Mountbatten Medal. He serves on the Technical Program Committee of various international conferences, including the European Microwave Conference.